EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L4	42	"BRICKELL, ERNIE"	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2007/11/25 13:24
L5	2	l4 and ("exponentiations" with ("prime" adj "number"))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2007/11/25 14:17
L6	34017	"INTEL CORPORATION"	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2007/11/25 13:56
L7	1	l6 and ("exponentiations" with ("prime" adj "number"))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2007/11/25 13:56
L8	154	("exponentiations" with ("prime" adj "number"))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2007/11/25 13:56
L9	5	l8 and ("exponent" with ("bit" adj "length"))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2007/11/25 14:25
L10	1757	380/277	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2007/11/25 14:16
L11	10	l10 and ("exponentiations" with ("prime" adj "number"))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2007/11/25 14:19
L12	1	l11 and ("exponent" with ("bit" adj "length"))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2007/11/25 14:19
L13	1	l11 and ((receiv$3 with request$3) with ("proof" or prov$3))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2007/11/25 14:19
L14	2583	380/28	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2007/11/25 14:18

L15	37	l14 and ("exponentiations" with ("prime" adj "number"))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2007/11/25 14:20
L16	3	l15 and ("exponent" with ("bit" adj "length"))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2007/11/25 14:20
L17	0	l16 and ((receiv$3 with request$3) with ("proof" or prov$3))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2007/11/25 14:20
L18	3033	380/30	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2007/11/25 14:19
L19	51	l18 and ("exponentiations" with ("prime" adj "number"))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2007/11/25 14:19
L20	3	l19 and ("exponent" with ("bit" adj "length"))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2007/11/25 14:23
L21	31	l18 and ((receiv$3 with request$3) with ("proof" or prov$3))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2007/11/25 14:22
L22	0	l21 and ("exponentiations" with ("prime" adj "number"))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2007/11/25 14:21
L24	103	"708/606"	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2007/11/25 14:21
L25	1	l24 and ("exponentiations" with ("prime" adj "number"))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2007/11/25 14:23
L26	0	l24 and ((receiv$3 with request$3) with ("proof" or prov$3))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2007/11/25 14:24
L27	333	708/491	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2007/11/25 14:23

EAST Search History

L28	11	l27 and ("exponentiations" with ("prime" adj "number"))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2007/11/25 14:25
L29	1	l28 and ("exponent" with ("bit" adj "length"))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2007/11/25 14:23
L31	0	l27 and ((receiv$3 with request$3) with ("proof" or prov$3))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2007/11/25 14:25
L32	104	708/518	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2007/11/25 14:25
L33	0	l32 and ("exponentiations" with ("prime" adj "number"))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2007/11/25 14:25
L34	0	l32 and ((receiv$3 with request$3) with ("proof" or prov$3))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2007/11/25 14:26

Web Images Video News Maps Gmail more ▾ Sign in

Google Patent Search BETA

exponentiations with mod P is a prime numbe | Search Patents | Advanced Patent Search
Google Patent Search Help

The following words are very common and were not included in your search: **with is a**. [details]

Patents

Patents **1** - **10** on **exponentiations with mod P is a prime number**. (**0.25** seconds)

Sort by relevance | Sort by date (new first) | Sort by date (old first)

Method and apparatus for protecting public key schemes from timing and fault ...
US Pat. 5991415 - Filed May 12, 1997 - Yeda Research and Development Co. Ltd. at the Weizmann Institute of Science
... the further improvement where j is chosen as a **prime number**. 6. ... since the small **exponentiations** in the 25 operation x"d (**mod** n) where n=**p***q, ...

RSA Public-key data encryption system having large random **prime number** ...
US Pat. 4351982 - Filed Dec 15, 1980 - Racal-Milgo, Inc.
Therefore, **p** and q must be large random **prime** num- transmission and receipt ...
this also requires a possibly compromisable physi- (**mod P**) for 100 random a ...

Verification of the private components of a public-key cryptographic system
US Pat. 6952476 - Filed Feb 8, 2000 - Hewlett-Packard Development Company, L.P.
... workload of 5k 2o **exponentiations mod P** into 5.5k **exponentiations mod** n. ...
to said second party a **number P** such that **P is a prime number** and nl(Pl); ...

Digital message encryption and authentication
US Pat. 6396928 - Filed Oct 24, 1997 - Monash University
mod p. Alice's signature on a message m is composed of two numbers r and s which
.... HASH = 1] EXP=the **number** of modulo **exponentiations**, MUL=the **number** of ...

High speed modular exponentiator
US Pat. 6282290 - Filed Mar 28, 1997 - Mykotronx, Inc.
... of smaller modular **exponentiations** together to provide respective first level
... **mod** q in which **p** and q are **prime** numbers having a product equal to n. ...

Method and apparatus for use in public-key data encryption system
US Pat. 4633036 - Filed May 31, 1984 - Martin E. Hellman
The signal representing the value **p mod** rs is applied as one of four input ...
LEN(r) are **prime**, the **number** of f values tested will be reasonable (eg, ...

Server-aided computation method and distributed information processing unit
US Pat. 5046094 - Filed Feb 2, 1990 - Kabushiki Kaisha Toshiba
Z = 1* **mod** n = S'lb **mod** n = Salb **mod** n = (S"*)' **mod** n = S" **mod** n = \P **mod** n 10
... Thus, when a **prime number** is selected for e, this attack method fails and ...

Device and method for calculating a result of a modular exponentiation
US Pat. 7248700 - Filed Feb 27, 2004 - Infineon Technologies AG
... with the modulus n into two modular **exponentiations** of second sub-moduli **p**,
... dq=d **mod**(ql), wherein q is a second **prime number**, wherein a product of **p** ...

Information security device, **prime number** generation device, and **prime** ...
US Pat. 7130422 - Filed Apr 12, 2002 - Matsushita Electric Industrial Co., Ltd.
L2, . . . , q **mod** Ln, to the **prime** generating unit 1016. ... then receives **prime**

p from **number** of 256-bit modular **exponentiations** performed to P1"™6 storing ...

Multiple **prime number** generation using a parallel **prime number** search algorithm
US Pat. 7120248 - Filed Mar 26, 2001 - Hewlett-Packard Development Company, L.P.
Athird curve 39 is for plotted values of percentage of **exponentiations** save for
... <xp-1=l(**mod.P**) () where **P is a prime number** candidate (eg, **P**=n0). ...

Gooooogle ▶
Result Page: 1 2 3 4 5 **Next**

exponentiations with mod P is a prime numb Search Patents

Google Patent Search Help | Advanced Patent Search

Google Home - About Google - About Google Patent Search

Web Images Video News Maps Gmail more ▾ Sign in

Google™ Patent Search BETA

exponentiations with h mod P | Search Patents | Advanced Patent Search
Google Patent Search Help

"with" is a very common word and was not included in your search. [details]

Patents

Patents **1** - **10** on **exponentiations with h mod P**. (**0.09** seconds)

Sort by relevance | Sort by date (new first) | Sort by date (old first)

Verification of the private components of a public-key cryptographic system
US Pat. 6952476 - Filed Feb 8, 2000 - Hewlett-Packard Development Company, L.P.
We nevertheless use a ten percent expansion and convert Bob's workload of 5k 2o **exponentiations mod P** into 5.5k **exponentiations mod** n. ...

Ideal electronic negotiations
US Pat. 5615269 - Filed Feb 22, 1996
8 Rather than obtaining type-2 values by evaluating **H** at inputs Vk that are ...
type xd **mod** n, where d is the multiplicative inverse of e **mod** (**p**-1) (q-1); ...

Digital message encryption and authentication
US Pat. 6396928 - Filed Oct 24, 1997 - Monash University
In practice, g is obtained by calculating g=\\(-**p**~1~>lq **mod p** where **h** is an integer
... DIV = 2 ADD = 0, HASH = 1] EXP=the number of modulo **exponentiations**, ...

Verification protocol
US Pat. 6446207 - Filed Jan 29, 1998 - Certicom Corporation
In a DSA signature scheme the signature components r and s are given by: r=(g^ **mod p**)**mod** q; and s=k~1(**h**(m)+dr)**mod** q where typically: 35 d is a random ...

Secure electronic voting using partially compatible homomorphisms
US Pat. 5495532 - Filed Aug 19, 1994 - NEC Research Institute, Inc.
Note that many modular **exponentiations** with the same base are being performed.
... ax **mod p** from 3Ak, to Vzk, requiring a table size of (n+2)k2 bits. ...

High speed modular exponentiator
US Pat. 6282290 - Filed Mar 28, 1997 - Mykotronx, Inc.
TT i-, . 'tiation of the same order as bp **mod p**, the inverse may be perform ...
of the two modular **exponentiations** may be data is provided to the data user. ...

Compact microelectronic device for performing modular multiplication and ...
US Pat. 5513133 - Filed Nov 18, 1993 - Fortress U&T Ltd.
Using a simple division calculation we know for comparison that t **mod** q=5c8. ...
B)NB ¥ (**P** (b • **H**)N (steps a and b are equivalent to B ¥ B2 modN) IF E(j) ...

Auto-recoverable and auto-certifiable cryptostem using zero-knowledge proofs ...
US Pat. 6282295 - Filed Oct 28, 1997
14. add (Q,, C^, C-2) to the end of **P** 15. val=**H**(**P**) 16. set b1,b2, ... (tt- raised to the a.fj- power) **mod** n=vJ-J-, where j=l+bj- The verifying system ...

Method, identification device and verification device for identificaiton and ...
US Pat. 5502764 - Filed Jan 24, 1994 - Thomson Consumer Electronics S.A.
RA2 **mod** X & m) and reads said number Z as a set {Cj, ,. . ,ch} of **h** numbers c

... algebraic function **P**. In this case the number Z is defined by Z=**H**(**P**(Rj2 &. ...

Compact microelectronic device for performing modular multiplication and ...
US Pat. 5742530 - Filed Dec 28, 1995 - Fortress U&T Ltd.
J0=7 as 7-9=-l **mod** 16 and **H**=2'12 **mod** a59=44b. The expected result is FsA-B **mod**
... **exponentiations** and multiplications this would be most efficient. ...

Gooogle ▶
Result Page: 1 2 3 **Next**

exponentiations with h mod P | Search Patents

Google Patent Search Help | Advanced Patent Search

Google Home - About Google - About Google Patent Search

Web Images Video News Maps Gmail more ▾ Sign in

Patent Search BETA

exponentiations with mod P a prime number | Search Patents | Advanced Patent Search
Google Patent Search Help

"with" is a very common word and was not included in your search. [details]

Patents

Patents **1** - **4** on **exponentiations with mod P â prime number**. (**0.29** seconds)

Sort by relevance | Sort by date (new first) | Sort by date (old first)

Did you mean: ***exponentiations with mod A prime number***

Information security device, **prime number** generation device, and **prime** ...
US Pat. 7130422 - Filed Apr 12, 2002 - Matsushita Electric Industrial Co., Ltd.
... modular **exponentiations** performed to P1"™6 storing unit 103 as **prime pa**. ...
Here, computational complexity of generating a **Prime** 1' 1 **mod** Li> q **mod** L2, ...

Multiple **prime number** generation using a parallel **prime number** search algorithm
US Pat. 7120248 - Filed Mar 26, 2001 - Hewlett-Packard Development Company, L.P.
Preferably, the in **prime number** generation performance of Multi-**prime** key **prime**
... pt are referred to as factors of the of **exponentiations** saved due to ...

Code exchange protocol
US Pat. 7016500 - Filed Mar 18, 1999 - Rohde & Schwarz SIT GmbH
By using the asymmetrical pair of codes SA, **PA** and SB, PB to form the session code
... The low **number** of 65 required **exponentiations** results in a decisive ...

Implicit certificate scheme
US Pat. 6792530 - Filed Sep 22, 2000 - Certicom Corp.
T then computes **PA**=a^A **mod** p. **PA** is A's KEY reconstruction public data, ...
the ID-based implicitly-verifiable public key needs two **exponentiations**. ...

exponentiations with mod P a prime number | Search Patents

Google Patent Search Help | Advanced Patent Search

Google Home - About Google - About Google Patent Search